A Study of Zero-Knowledge Proof

Priyanka Ghosh
Computer Science &Engineering
Brainware University Kolkata,India,
aecpriyanka@gmail.com

Dr. Rajdeep Chakraborty
Computer Science Engineering
Netaji Subhas Engineering college
India rajdeep.chak@gmail.com

Sherya Singh
Computer Science &Engineering
Brainware University
singhshreya747392@gmail.com

Abstract

Data is the new language of the 21st century. The dependency on the digital world has increased by many folds compared to the last few decades. During the pandemic, the world has now learnt to survive and stay connected with the help of technology and the digital world. With this increasing dependency on data, the need for security is also becoming critical and the conventional techniques of authentication seem ineffective with the increasing variety of security requirements. The Zero-knowledge proof technique is an authentication technique where the prover or the verifier does not need to disclose any information to complete the authentication process. This ensures that neither the prover nor the verifier can do misuse the secret information. The application of this technique can be in a variety of fields where data security is at higher priority. This ZKP technique has advantages over the traditional public-key techniques. Through the Zero-Knowledge Proof technique, a higher degree of reliability and robustness can be achieved.

Keywords—Zero knowledge proof, Authentication, IoT, security, Lightweight cryptography

INTRODUCTION

The Internet of Things (IoT) emerged as a new era of application in almost all fields of society and engineering problems. In all applications of IoT, sensors are deployed to form a network to observe the physical or natural condition and can collaborate with other components of the system to keep a record of the status of things such as movements, temperature, heat, pressure, humidity, etc. Internet of Things means a combination of two terms: first is the Internet, the Internet means a network where billions of computing devices connected and communicate by some common rules is called protocols. The second is the Things, which means these devices and objects are converted into intelligent objects where each device can communicate, compute, and converted into meaningful information as to their requirement. In other words, IoT is the interconnection of physical worlds (sensors and actuators) and digital worlds. The IoT simply refers to the expansion of computation and network capabilities to not only computers and mobile phones but also various devices and sensors in the world [1]. IoT devices has already outnumbered the number of people in the workplace [2], and the number of wireless devices connected to the Internet of Things will be about 26 billion by 2020 and will greatly outnumber hub devices (smart phones, tablets and PCs) [3] Security obstacles like privacy, secure communication, access control, safe storage of data are becoming important tackles in the IoT domain. IoT technology is facing problems from numerous security issues. Compare to other standard technologies. The security of information has now become the utmost priority for the users as breach of information may cause significant losses to individuals and organizations. To ensure the security and privacy of information, Zero Knowledge Authentication technique will play a vital role. Zero knowledge proofs are cryptographic protocols which do not disclose the information or secret itself during the transaction or authentication process

The Zero Knowledge Proof technology proposes a technique which employs cryptographic algorithms so that various parties can verify the validity of an item of information without sharing the exact data that composes it. This is a series of cryptographic algorithms through which a tester can mathematically demonstrate to a verifier that a computational statement is correct without revealing any data. This will prevent access of user information from the third party which in turn will keep the data privacy intact. For example, a user could declare that he is of the appropriate age to access a product or service, without revealing his actual age, or a person could prove that his income status to buy a product or service, without having to share the exact amount of money in his possession.

The State Of Art In Iot Security With Zero-Knowledge proof

The IoT can be considered both a dynamic and global networked infrastructure that manages self-configuring objects in a highly intelligent way. This, in turn, allows the interconnection of IoT devices that share their information to create new applications and services which can improve human lives [5]**.** Originally, the concept of the IoT was first introduced by Kevin Ashton, who is the founder of MIT auto identification center in 1999 [5][6]. Ashton has said, "The Internet of Things has the potential to change the world, just as the Internet did. Later, the IoT was officially presented by the International Telecommunication Union (ITU) in 2005 [7]. The IoT has many definitions suggested by many organizations and researchers. In addition, Guillemin and Friess in [8] have suggested one of the simplest definitions that describe the IoT in a smooth manner. It stated: "The Internet of Things allows people and things to be connected Anytime, Anyplace, with anything and anyone, ideally using any path/network and any service". IoT has the equivalent issues furthermore it has additional security mechanisms such as information storage, different authentication processes, privacy issues and access control and network management so on. Among these list data security and privacy protection are major challenges in modern IoT system moreover these mechanisms decide the future growth of IoT appliances [9]– [11].

In IoT, both Radio Frequency Identification Devices (RFID)and Wireless Sensor Networks (WSNs) assure integrity and on identicality of information through cryptographic password technology. IoT expansion expeditiously rising in distinctive fields outset from smart devices to smart cities, smart society and internet of Everything (IoET), Battlefield- based IoT (IoBT), Internet of medical things (IoMT), improvement smart grids, etc. Moreover, fields like IoMT and IoBT which consists of data-flexibility appliances ensure the security of devices, systems moreover data computing is decisive [12]– [15].

Definition of ZKP

Zero knowledge proof model of computational defined as an interactive proof system (P, V), where P is a prover and V isa verifier. Protocol () is for proving language membership statement for a language over {0,1}. Let a L be a language over {0,1}*, for a membership instance x ϵ L, P and V must share the common input x, proof instance is denoted as (P, V) (x).P and V are linked by a communication channel over which exchange a sequence, called proof transcript a1, b1, a2,b2….an, bn.

Zero Knowledge Proof (ZKP), a set of tools that allow an item of information to be validated without the need to expose the data. The main essence behind this concept is to prove possession of knowledge without revealing it.

- **Completeness:** If the statement is really true and both users follow the rules properly, then the verifier would be convinced without any artificial help.
- **Soundness:** In case of the statement being false, the verifier would not be convinced in any scenario. (The method is probabilistically checked to ensure that the probability of falsehood is equal to zero)
- **Zero-knowledge:** The verifier in every case would not know any more information.

Actually, Zero Knowledge proof Protects data from criminals, and in some cases, the government, Replaces the risky nature of password-only authentication, keeps online payments and transactions safe, Ensures the validity of block chains, Secures public cloud accounts. Now the question is how is this possible? In the academic world there is a simple example is often used to illustrate the logic maintained by a cryptographic algorithm that makes this technology possible: 'The cave of Ali Baba'. Let's imagine that two characters, Alice and Bob, find themselves at the opening of a cave which has two distinct entrances to two separate paths (A and B). Inside the cave there is a door that connects both paths, but can only be opened with a secret code. Bob (the 'tester') owns this code and Alice (the 'verifier') wants to buy it, but first she wants to be sure that Bob is not lying. How can Bob show Alice that he has the code without revealing its contents? To achieve this, they do the following: Alice waits outside the cave and Bob enters at random through one of the doors (A or B). Once inside, Alice approaches the entrance, calls Bob and asks him to exit through one of the two paths. As Bob has the secret code, he will always be able to return via the path that Alice asks him to, even though it may not coincide with the path he has chosen in the first place, as in this case he can open the door and exit through the other side.

Zero knowledge is effective as well in case of goods privacy and security in block chain oracles. These IT tools allow'smart contracts' to update their status, with the incorporation of external information from verified sources in order to trigger scheduled orders or events. In these cases, ZKP could facilitate the implementation of these systems guaranteeing, at the same time, the privacy of external data that should interact with the block chain in permitting a scheduled action to be triggered, without the need to share the data itself.one of the benefit of Zero knowledge is its secure more than other technology. IT is takes vital part in case of IoT security. A lot of research works have discussed about security related problems, like Security issues in the wireless sensor networks (WSNs), DoS attack on different layer, Security issues in RFID technology. Security issues, such as privacy, authorization, verification, access control, system configuration, information storage, and management, have been the main challenges in an IoT environment.

Zero Knowledge Proof technique by which one party (prover) can prove to another party (verifier) without disclosing of any information apart from the fact. If IoT security can be developed using Zero knowledge proof, then it would help to enhance the level of security significantly for billions of connected devices which have made the IoT heterogeneous in nature. With this technique messages are passed from object to object without revealing any information in the network. This ensures the privacy in the middle of the execution that no information is leaked to the attacker.

Comparative Study

Diffie-Hellman (D-H) key exchange algorithm is known as one of the earliest practical instances of Zero-Knowledge Protocol where two sides share one non-private communication channel to interact and the authentication process takes place without sharing any secret information. No side will require any prior information to authenticate and the transaction lefts no traces of the secret information. Each side uses a common shared key which is a symmetric key cipher to encrypt the communications.

Quite possibly the most entrancing employments of zero-information evidence inside cryptographic conventions is to uphold legit conduct while looking after protection. Generally, the thought is to authorize a client to demonstrate, utilizing a zero-information verification, that its conduct is right as indicated by the convention. Due to adequacy, it is realized that the client should truly act really to have the option to give a legitimate confirmation. Due to zero information, it is evident that the client does not bargain the protection of its privileged insights during the time spent giving the confirmation [11, 12].

Fiat-Shamir ZKP Protocol

In Fiat-Shamir ZKP protocol, it satisfies the condition of zero knowledge, where the two par- ties (prover and verifier) complete the authentication process without any prior knowledge and sharing the secret information. The prover focuses on proving that it holds the secret information and does not need to reveal it for authentication process [13]. In Fiat-Shamir protocol, a trusted third party chooses to large random numbers, p and q and calculates n (n = p * q). The third party reveals the value of n as public key while keeping the value of p and q secret. Figure 8.2 illustrates the transactions take place in the process. The prover P and verifier B follows the below mentioned steps to complete the process [21].

1. The prover Alice (P) chooses a random number r and calculates {$x = r^2$ mod n}, where n is the shared public key.

2. Alice shares the value of x with the verifier Bob (b) as witness.

3. Bob chooses a number between 0 and 1 and sends it as challenge (C) to Alice.

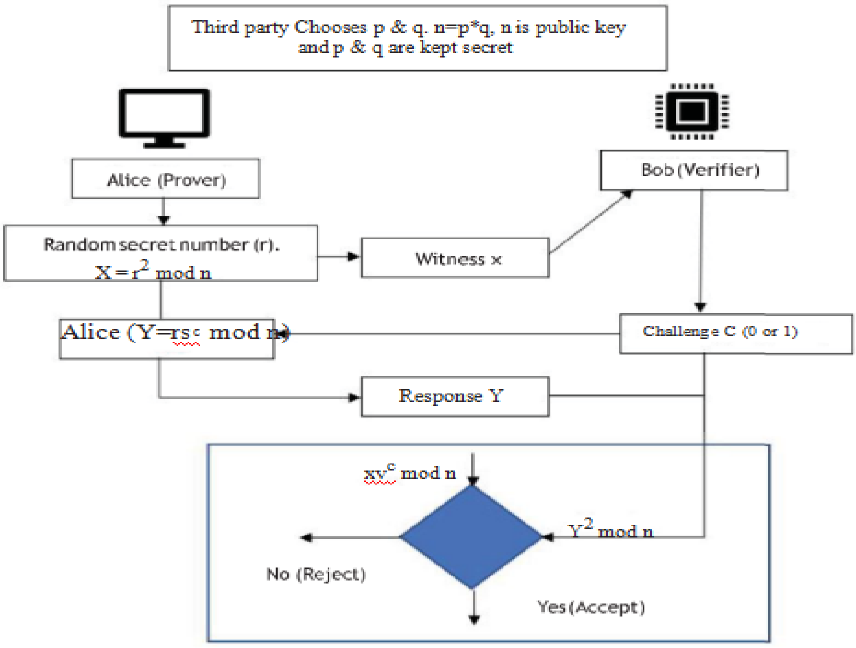
4. With the help of value of C, Alice calculates Y {$Y = r^2$ mod n}.
5. Alice shares the Y with Bob as response to the challenge.

6. Bob the verifier calculates Y^2 mod n and xv^c mod n.
7. Bob compares both the values, if they are same, then Alice is authentic; otherwise, Bob considers this as a failure of authentication.

8. The process gets iterated for one to six times with different values of C as 0 or

1. The prover needs get through every time to prove its authenticity.

   There is another similar protocol as Feige-Fiat-Shamir protocol, which follows a series of private keys and public key and array of challenges for the authentication process.



Diffie-Hellman Key Exchange Algorithm

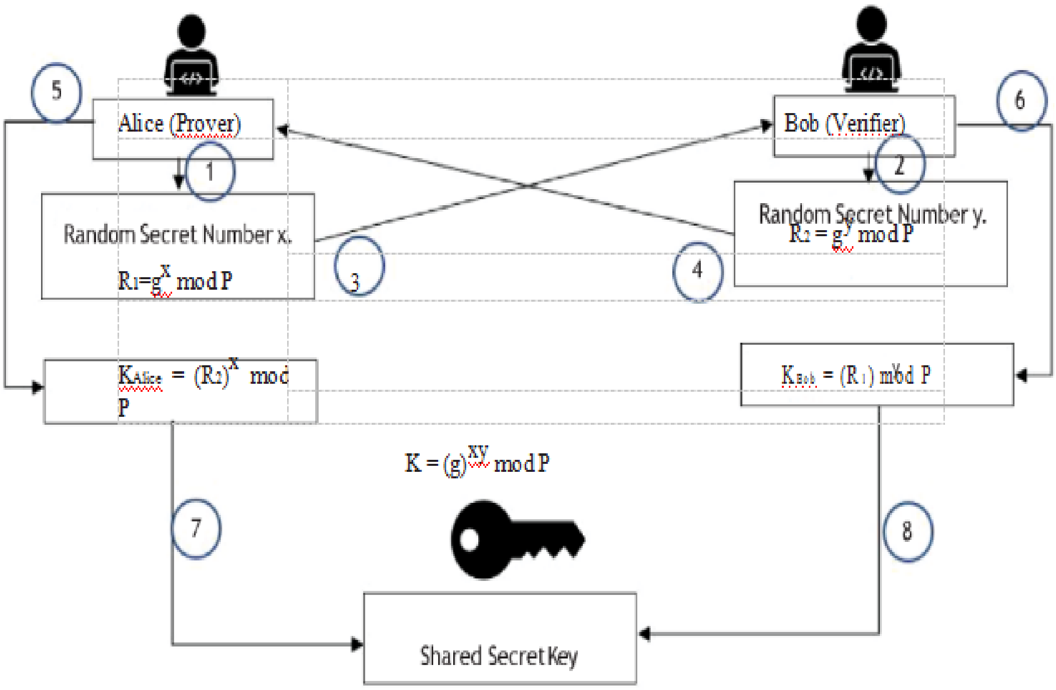
D-H key exchange program was conceptualized in 1976 by Whitfield Diffie and Martin Hellman, which was the first practical ZKP protocol. Here, the prover and the verifier establish communication over a public communication channel and performs a set of mathematical transactions to authenticate the prover without revealing the secret. This algorithm uses multiplicative group of integers modulo p(Zp*, x), where P is a prime number, and 1 to p − 1 is used for different mathematical operations. The two parties choose random value of p and g. g is a primitive root in the group. The value of p and g are made public and follows the procedure as shown in Figure 8.3 [14, 20, 21].

1. Alice chooses a random value for x between 0 and p and calculates R = g^x mod p.
2. Bob the verifier picks up another random value for y and calculates R2= g^y 1 mod p.

3. Bob and Alice exchange R1 and R2.

4. Bob and Alice decode and calculate KAlice, Kbob, respectively.

The D-H key exchange algorithm is prone to “man-in-the-middle” and “discrete algo- rithm” attacks [6]. These operations of these two attacks are described as below.



Techniques	Interaction technique	Third party involvement	Possible threats	Encryption technique	Operating technique	Limitations
Fiat-Shamir ZKP Protocol	Exchange Challenge and witness	Yes	Discrete logarithm attack and man-in- the-middle attack	No	Utilizations measured number juggling and equal check measure	Repetitive and infeasible
Diffie-Hellman Key Exchange Algorithm	Exchange keys	No	Discrete logarithm attack and man-in-middle attack	No	Utilizations a multiplicative gathering of whole numbers module	Infeasible due to technical complexity

Conclusion

This paper a survey has been conducted on Zero Knowledge proof. There are very less efforts have been made to implement Zero Knowledge proof technique in IOT for security enhancement. Zero Knowledge proof has advantages over the public key protocols and other authentication tools and can be implemented over a wide range of applications. In this technique user will not have to share any information even to the source, which ensures other than the key holder, no one has the keys to access the data.

References

1. Atlam,H.F.,Walters,R.J.,Wills,G.B.(2018)Internet of Things: State-of-the-art, Challenges, Applications, and Open Issues . *Int. J. Intell. Comput. Res. 9*(3), 928–938.
2. Federal Trade Commission. (2015). *Internet of Things: Privacy & Security in a Connected World*. Retrieved from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
3. Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020 - Attivo Networks. (2013, December). Retrieved from : https://www.attivonetworks.com/gartner-says-the-internet-of-things-installed-base-will-grow-to-26-billion-units-by-2020/

4. Atlam, H.F, Alenezi, A., Walters, R.J., Wills, G.B., Daniel, J.(2017). *Developing an adaptive Risk-based access control model for the Internet of Thing*s.2017 IEEE International Conference on Internet of Things (I Things) and IEEE Green Computing and Communications (Green Com) and IEEE Cyber, Physical and Social Computing (CPS Com) and IEEE Smart Data.

5. R. Shanbhag and R. Shankarmani.(2015). Architecture for Internet of Things to minimize human intervention.*2015Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2015*.

6. G. Joshi and S. Kim.(2013). Survey, Nomenclature and Comparison of Reader Anti-Collision Protocols in RFID. *IETE Tech. Rev.*,*25*(5), 285 .

7.The Internet of Things 2005. (2005). Retrieved from https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf

8. P. Guillemin and P. Friess. (2009).Internet of Things Strategic Research Roadmap. *Eur. Comm. Inf. Soc. Media.*

9. Akyildiz, I.F., Su, W., Sanakarasubramaniam, Y., Cayirci, E. (2002). Wireless sensor networks: asurvey. *Comput. Netw. 38*(4), 393–422.

10. Hamad, F., Smalov, L., James, A. (2009).Energy-aware security in M- Commerce and the internet Of things. *IETE Tech. Rev. 26*(5), 357–362

11. Tsudik, G.: YA-TRAP: yet another trivial RFID authentication protocol. In: Proceedings of Fourth Annual IEEE International Conference on Pervasive Computing and CommunicationsWorkshops, pp. 196–200 (2006)

12. Da Costa Júnior, E.P.: An Architecture for Self-adaptive Distributed Firewall

13. Li, B., Lu, R., Wang, W., Choo, K.-K.R. (2017). Distributed host-based collaborative detection for false data injection attacks in smart grid cyber physical system. *J. Parallel Distrib. Comput.103*, 32–41

14. Almotiri, S.H., Khan, M.A., Alghamdi, M.A.(2016). *Mobile health (m- Health) system in the context of IoT*. In: 2016 IEEE 4th International Conference on Future Internet of Things and CloudWorkshops (FiCloudW), Vienna.

15. Grigoriadis C, Papastergiou S, Kotzanikolaou P, Douligeris C, Dionysiou A, Elias A, Bernsmed K, Meland P and Kamm L.(2021). *Integrating and Validating Maritime Transport Security Services: Initial results from the CS4EU demonstrator*. 2021 Thirteenth International Conference on Contemporary Computing (IC3-2021).

16. Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., and Carle, G. (2013).DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Networks, 11*(8), 2710–2723.

17. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., and Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. W*ireless Networks, 20*(8), 2481–2501.

18. Tsai, C.-W., Lai, C.-F., and Vasilakos, A. V. (2014). Future Internet of Things: open issues and challenges. *Wireless Networks, 20*(8), 2201–2217.

19. Pongle, P., andChavan, G. (2015). *A survey: Attacks on RPL and 6LoWPAN in IoT*. 2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015.

20. Evans, D. (2011). Cisco Internet Business Solutions Group (IBSG) The Internet of Things How the Next Evolution of the Internet Is Changing Everything. Retrieved from https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

21. Weissberger ,A.(2017) .*IoT Forecast, 5G & Related Sessions*. In: IDC Directions Conference, Santa Clare